LISTING OF THE CLAIMS

What is claimed, is:

1. (Currently amended)) A communications monitoring system comprising:

a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and

a similarity calculator for calculating formal similarity between two packet streams of similar duration composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion.

2. (Original) The communications monitoring system according to Claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other.

3. (Original) The communications monitoring system according to Claim 1, wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator.

4. (previously presented) A communications monitoring system comprising:

a packet input means for receiving communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and

matching means for performing real-time matching between two packet streams composed of communications packets received by the packet input means and employing said real-time matching in detecting an intrusion.

5. (Currently amended) The communications monitoring system according to Claim 4, wherein the matching means determines formal similarity between the two packet streams being similar in an amount of data and transmission interval of packets irrespective of data content and is determined based on a time lag between each corresponding pair of communications packets in the two packet streams.

6. (Original) The communications monitoring system according to Claim 5, further comprising alerting means for sending out a predetermined alert according to the formal similarity between the two packet streams determined by the matching means.

7. (Currently amended) A communications monitoring method for monitoring data communications using a computer, comprising the steps of:

acquiring in real time communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications being any of communications conducted via a host and communications conducted directly;

on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means;

determining formal similarity between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong, said second packet stream being of similar duration of said first packet stream; and

sending out a predetermined alert according to the determined similarity.

8. (Original) The communications monitoring method according to Claim 7, wherein in the step of determining the formal similarity of packet streams, the formal similarity between the two packet

streams is determined based on a time lag between each corresponding pair of communications packets in the two packet streams.

9. (Original) The communications monitoring method according to Claim 7, further comprising a step of discarding information used in determining the similarity of second packet streams except the second packet stream determined to be most similar to the first packet stream.

10. (Currently amended) An information processing method comprising comparing two packet streams flowing in real time on a network, the step of comparing comprising the steps of:

acquiring communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications packets being in any of communications conducted via a host and communications conducted directly;

on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; and

performing matching between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong, wherein said second packet stream being of similar duration of said first packet stream.

11. (Original) The information processing method according to Claim 10, wherein in the step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other.

12. (Original) The information processing method according to Claim 11, wherein in the step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs.

13. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 7.

14. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for communications monitoring, said method steps comprising the steps of claim 7.

15. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing information processing, the computer

readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 10.

16. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for information processing, said method steps comprising the steps of claim 10.

17. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1.

18. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 4.

19. (Currently amended) ~~2.~~ The communications monitoring system according to Claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two

graphs when the graphs of the packet streams are moved close to each other without intersecting each other, and

wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator. ~~calculator.(~~

20. (previously presented) The information processing method according to Claim 10, wherein in the step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, and

wherein in the step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs.